« Je n’ai rien à cacher. Ou peut-être que… »

La sécurité des données, ça vous parle ? Le sujet, souvent pris à la légère en France, mérite pourtant toute l'attention du grand public. Maxime Huber, cofondateur de la startup Seald, revient dans un post Medium sur l'intérêt de crypter ses données personnelles.

Souvent, lorsque je parle de mon projet et de l’utilité de la cryptographie, la réponse que l’on me donne est “Je n’ai rien à cacher!”

Cette réponse implique que seules les personnes ayant des secrets ou pratiquant des activités illégales, sont susceptibles d’être intéressées par la cryptographie. Êtes-vous sûr que ce soit le bon raisonnement ?

Essayez de demander à ces personnes qui n’ont rien à cacher de vous donner leur code de carte bleue ou leurs mots de passe sur internet, ils comprennent soudainement l’intérêt de la cryptographie comme un garant de leur confidentialité.

Aujourd’hui, la cryptographie est utilisée aussi bien dans le domaine professionnel que dans le domaine privé. Elle est déjà indispensable pour un bon nombre d’entre nous, mais doit aller plus loin: des outils de cryptographie simples à utiliser sont une étape nécessaire pour sécuriser complètement notre vie sur internet.

C’est incroyablement puissant

L’armée a commencé à utiliser le chiffrement pour empêcher les ennemis de comprendre les communications en cas d’interception. Ensuite, le chiffrement de données s’est étendu aux domaines professionnels, par exemple dans des entreprises avec une forte composante industrielle ou scientifique voulant se protéger de l’espionnage industriel.

Mais depuis la seconde guerre mondiale, les besoins en cryptographie ont explosé. Ses applications civiles sont maintenant très nombreuses.

Vous l’utilisez tous les jours

Entrer un code PIN ou un mot de passe sur internet ou dans un distributeur, utilise déjà de la cryptographie. Petit à petit, elle a envahi notre quotidien mais de manière transparente et facile d’usage.

Lorsqu’une carte de crédit est insérée dans un distributeur ou un terminal de paiement, de nombreuses vérifications de données chiffrées sont effectuées: notamment pour vérifier que vous avez entré le bon code, que le numéro de carte correspond bien à votre compte, etc. Tout cela pour valider un paiement ou un retrait (enfin, si vous avez de l’argent).

Il est très pratique de pouvoir acheter en ligne. Nous le faisons tous car la plupart du temps, le processus de paiement est sécurisé. Mais lorsque vous communiquez vos mots de passe, votre numéro de carte ou toute autre donnée sensible sur Facebook, Gmail, Outlook, Messenger… ils ne doivent pas passer en clair (non chiffrés) sur le service.
Vous ne voulez pas que votre numéro de carte soit transmis à tout le monde et qu’il soit utilisé pour dépenser votre argent, moi non plus !

Voilà pourquoi des protocoles de cryptographie on été mis en place : pour empêcher ces vols en ligne.

> *« Dire que vous ne vous souciez pas du droit à la confidentialité parce que vous n’avez rien à cacher revient au même que de dire que vous ne vous souciez pas de la liberté d’expression parce que vous n’avez rien à dire »*
> – Edward Snowden

Ce n’est pas automatique partout

Qu’en est-il de vos conversations quotidiennes ? De votre compte Facebook ? De tous vos e-mails ? De tous les outils et plateformes de communications que

vous utilisez ?

Faites-moi confiance, vous n'êtes pas en sécurité… Il est très facile d'avoir accès à tout cela (keylogger, phishing, utiliser le mot de passe que vous avez écrit sur un papier, …), de lire toutes vos conversations et d'utiliser vos données privées. Comment est-il possible de vous en protéger ?

Une question que des spécialistes du domaine (à l'image de Seald) essaient de régler chaque jour, en rendant les conversations faciles à sécuriser. L'idée de la startup : permettre à chacun de chiffrer de bout en bout (avec RSA-4096 et AES-256) tous ses messages, documents, posts sur les services qu'il utilise déjà (Facebook, Slack, Gmail, Messenger, …), en sélectionnant seulement quelques destinataires capables de déchiffrer et lire les messages envoyés.

Retrouvez le post original de Maxime Huber sur Medium